Networks, Security, and Protection

5

29
COMPUTER NETWORKS: LANs, MANs, WANs, AND WIRELESS 465

Introduction 465
Computer Networks 465
- Packet-Switched Networks 465
- Configurations of Communication Services 466
- Point-to-Point Communications 466
- Multicasting Communication 466
- Broadcasting Communication 466

Classes of Computer Networks 466
- Local Area Network 466
- Metropolitan Area Network 467
- Wide Area Network 467

Local Area Network Standardization 467
LAN Architecture: Open System Interconnection-Reference Model 467
- Protocols: Interfacing in LAN Layer 469
- Layered Protocol Configurations 470
- LAN Topology and Connectivity 470
- NetWare Operating System 471

Metropolitan Area Networks 472
Wide Area Networks 473
- Applications of WANs 474
- WAN-Based Technologies 475

Internet Protocol Networks 476
- Variations of IP Networks 476

Personal Area Network 476
Client–Server Model and Socket Programming 476
- Socket 477
- Socket Implementation Issues 477
- Client–Server Implementation Using Socket 478

Wireless Networks and Security Issues 478
- Components of Wireless Networks 478
- Advantages and Disadvantages of WLANs 479
- Configurations in Wireless LANs 480
- WLAN Standardization 480
- Standard Protocol for Wireless LANs 480
- Wireless Technology Types 481

Security Issues in WLANs 481
- Unauthorized Access and Attacks 481
- Security Standardization in WLAN 482
- RF Shielding 482

References 482

30
INTERNET FUNDAMENTALS AND CYBER SECURITY MANAGEMENT 484

Introduction 484
What Is Internet? 484
Evolution of Internet 485
- World Wide Web 487
- Forms of Web Document 487

Host Configuration 487
TCP/IP Protocol Suite 488
Internet Protocol Addressing 490
- Classes of IP Addressing 490

© 2012 by Béla Lipták

Internetworking Protocol Version 6 491
IPSecurity 491
Domain Name System 491
Dynamic Domain Name System 492
Routing Protocols 492
Unicast Communications 492
Multicasting Communication 492
Real-Time Interactive Services over Internet 492
Protocols for Real-Time Interactive Applications 493
Internet Service Providers 493
Internet Standardization 494
Standards Organizations, Forums, and Regulating Agencies 494
Cyber Security and Security Management 495
Cyber Attack Tools and Well-Known Attacks 495
Hidden Threats 497
Phishing and Pharming 498
Targeted Cyber Attacks 498
Security Concerns 498
Cyber Security Management 498
Measures against Cyber Attacks 498
Network Infrastructure for Cyber Security 499
Use of Network Framework for Cyber Security 499
Security Measures for Network Infrastructure 500
Penetration Testing and Security Auditing 502
Cryptography 502
Digital Signature 502
Minimizing Impact—Detecting the Attack 502
Incident Response Team 502
Containment 503
Responding to Cyber Attacks 503
Develop Mechanisms to Respond to Cyber Incidents Leading to Cyber Attack 503
Cyberethics 503
Cyberspace Regulation 504
Cyber Standards Organizations 504
Acknowledgments 504
References 504

31
NETWORK SECURITY, THREATS, AUTHENTICATION, AUTHORIZATION, AND SECURING DEVICES 506

Introduction 506
Private Key Encryption 506
Stream Ciphers 507
Block Ciphers 507
Public Key Encryption 508
Data Encryption 508
RSA versus Elliptic Curve Cryptography 508
Public Key Infrastructure 508
Recent Developments 509
Threats 509
SQL Injection 510
Phishing 510
Pharming 510
Authentication 510
Password Authentication 510
Certificate Authentication 511
Token-Based Authentication 511
Biometrics-Based Authentication 511
Authorization 512
Basic File Permissions in Linux 512
Advanced Permissions in Linux 512
Access Control Lists, Capabilities, and File Attributes in Linux 513
Securing Devices 513
Full Disk Encryption Tools 513
An Example: Disk Encryption in Linux 515
Conclusions and Summary 515
References 516

32
VPN, CCN, AND IT SUPPORT 517

Introduction 517
Characteristics of VPNs 517
Types of VPNs 518
Remote-Access VPN 518
Client-Based VPNs 518
SSL-Based VPNs 518
Secure Socket Layer 518
Identifying SSL-Based Websites 518
SSL VPN Tunnels 519
SSL Reverse Proxy 519
Site-to-Site VPNs 519
VPN Tunnels and Protocols 519
IPsec 519
IPsec Features 520
IPsec Protocols 520
Internet Key Exchange 521
IKE Phase 1 521
IKE Phase 1.5 521
IKE Phase 2 521
Authentication Header 521
Encapsulating Security Payload 521
Encryption Algorithms 521
Symmetric Encryption 522
Asymmetric (Public Key) Encryption 522
Managing VPNs 523
Small- and Medium-Size Companies 523
Global Companies and Complex Communication Networks 523
Auto-Managed Networks 523

© 2012 by Béla Lipták

Service Delivery 523
Conclusions and Comments 523
References 523
Bibliography 524

33
FIBER-OPTIC NETWORK COMPONENTS 525

Introduction 525
Optical Networks 525
History of Optical Communication 525
Modern Optical Communications 525
Networks 527
Network Types 527
Protocols and Services 527
Information Channels and Transport 528
First-Generation Optical Networks 528
Access Schemes 529
Topologies 530
Current Optical Networks 532
Next-Generation Optical Networks 532
Optical Fibers 532
Attenuation and Loss 533
Dispersion 534
Nonlinearities 534
Light Sources 535
Optical Receivers 536
Optical Switches 536
Microelectromechanical Systems 537
Acousto-Optic 537
Electro-Optic 537
Thermo-Optic 537
Magneto-Optic 537
Multiplexers/Demultiplexers 538
Amplifiers 539
Erbium-Doped Fiber Amplifiers 540
Raman Amplifiers 540
Semiconductor Optical Amplifiers 540
Passive Components 541
Power Splitters/Couplers 541
Isolators/Circulators 541
Other Systems 542
Regeneration 542
Wavelength Conversion 543
References 543

34
FIBER-OPTIC COMMUNICATIONS AND NETWORKS 546

Summary 546
Introduction 546
Reconfigurable Add–Drop Multiplexer and Optical Cross-Connect 546
Optical Add–Drop Multiplexer 547
Reconfigurable Optical Add–Drop Multiplexer 547
Optical Cross-Connect 547
Waveband Switching 548
Multigranularity Optical Cross-Connect 548
Waveband Grouping 549
TDM Switching and Grooming 549
Photonic Slot Routing 550
Photonic Slot 550
Contention Resolution 551
Optical Flow Switching 552
Tell-and-Go Reservation 553
Reverse Reservation 553
Optical Burst Switching 553
OBS Network Edge 554
Burst Assembly 554
Signaling 554
Routing and Wavelength Assignment 555
Offset 555
OBS Network Core 555
Scheduling 556
Contention Resolution 556
OBS Medium Access Control Layer 556
Optical Packet Switching 556
Packet Format 557
Switch Architecture 558
Contention Resolution 559
Buffering 559
Wavelength Conversion 560
Unified Contention Resolution 561
Packet Optical Transport Network 561
Ethernet Frame 562
Provider Backbone Bridge-Traffic Engineering 563
Conclusions 563
References 564

35
NETWORK ACCESS PROTECTION 565

Introduction 565
Access Protection Models 565
Bell Padula Model 565
Access Control Lists 566
Capabilities 566
Role-Based Access Control 567
Resource Hierarchy 567
Policy-Based Access Control 567
Network Access Protection 568
Generic Access Protection Architecture 568
Example Instance: Network Access Control 569
Example Instance: NAP in VISTA 569
Conclusions and Comments 570
Bibliography 570

© 2012 by Béla Lipták

36
COMMENTS ON CYBER SECURITY IN INDUSTRIAL CONTROL SYSTEMS AND AUTOMATION 571

Overview 571
Partial Practical Examples 572
Conclusions 574
Reference 574

© 2012 by Béla Lipták